



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/544,493	04/07/2000	Sherman Janes	004698.P001	1791

7590 01/29/2004

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
1300 I Street, N.W.
Washington, DC 20005

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 01/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/544,493

Applicant(s)

JANES, SHERMAN

Examiner

Pramila Parthasarathy

Art Unit

2133

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) 12 and 25 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11, 13-24 and 26-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) #6.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1 – 11, 13 – 24, and 26 - 28 are presented for examination. Claims 12 and 25 have been cancelled.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2.1 Claims 1 – 11, 13 – 24, and 26 – 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baser (U.S. No. 6,170,061) in view of Mashayekhi (U.S. Patent No. 5,818,936).

As per Claims 1, 14, 19, Baser discloses that
receiving data from a network application program interface (API) (Col.35 Lines 23 – 25);
determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data (Col.22 Lines 50 – 52);
creating a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association (Col.3 Lines 22 – 29);

sending the data to which the security operation has been applied to a network protocol layer (Col.28 Lines 32 - 33).

Baser does not disclose that applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data. However, Mashayekhi discloses applying the security operation to the data (Col.3 Lines 37 - 39). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by applying the security operation using the security association as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

As per Claims 2, 15, 21, Baser does not disclose that using said selector to search a database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector. However, Mashayekhi discloses using selector to search a database of security associations (Col.7 Lines 54 - 57).

As per Claims 3, 16, Baser discloses that

the selector data is based [[on]] at least in part on one of an internet protocol address taken from the data and a port indicator taken from the data (Fig.6 #130).

As per Claims 4, 17, Baser discloses that

attaching a header to the data, said header including a security operation tag (Col.3 Line 50);
performing an integrity check (Col.4 Lines 1 - 3);

Baser does not disclose encrypting the data. However, Mashayekhi discloses key pair encrypts/decrypts (Col.6 Lines 57 - 59). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by encrypting the data as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

As per Claims 5, 18, Baser does not disclose that

determining if the data is eligible for the security operation and applying the security operation if the data is eligible depends, at least in part, upon a local selector/security association pair at a sending client corresponding to a remote selector/security association pair at a receiving client, said local selector/security association pair and said remote selector/security association pair having been received from a key server. However, Mashayekhi discloses that a local selector/security association pair at a sending client corresponding to a remote selector/security association pair having been received from a key server (Col.7 Lines 54 - 56 and Fig. 4A & 4B).

As per Claim 6, Baser discloses that

receiving data from a network protocol layer (Col.35 Lines 23 - 25);

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data (Col.22 Lines 50 - 52);

creating a selector based on the selector data, said selector indicating at least a portion of the data and a security association (Col.3 Lines 22 - 29);

sending the data to which the security operation has been applied to a network application program interface (API) (Col.28 Lines 32 - 33).

Baser does not disclose that applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data. However, Mashayekhi discloses applying the security operation to the data (Col.3 Lines 37 - 39). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by applying the security operation using the security association as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

As per Claim 7, Baser discloses that

detecting a security operation tag in a header to the data (Col.3
Line 50 and Col.9 Lines 30 - 32);
performing an integrity check (Col.4 Lines 1 - 3);

As per Claim 8, Baser does not disclose that

using said selector to search a database of security associations
for at least one selector/security association pair identifying a
security association corresponding to the selector. However,
Mashayekhi discloses using selector to search a database of security
associations (Col.7 Lines 54 - 57).

As per Claims 9, 22, Baser does not discloses that

blocking the data from being sent to the network API if no
security association corresponding to the selector is found. However,
Mashayekhi discloses blocking the data from being sent to the
network API if no security association corresponding to the selector
is found (Col.7 Lines 52 - 67).

As per Claim 10, 23, Baser does not discloses that

determining that the data is not eligible for the security
operation if a selector that references a database of security
associations cannot be created based on the data. However, Mashayekhi
discloses determining that the data is not eligible for the security
operation if a selector that references a database of security
associations cannot be created based on the data (Col.7
Lines 52 - 67).

As per Claim 11, 24, Baser does not discloses that

blocking the data from being send to the network API if the data
includes selector data but no selector can be created from it.
However, Mashayekhi discloses determining that the data is
blocked from being send to the network API if the data includes
selector data but no selector can be created from it (Col.7 Lines 52
- 67).

As per Claims 13, and 26 Baser does not disclose

applying encryption to the data; However, Mashayekhi discloses key pair encrypts/decrypts (Col.6 Lines 57 - 59). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by encrypting the data as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

Baser discloses that removing special packaging from the data (Col.9 Lines 30 - 31);

Baser does not disclose applying decryption to the data. However, Mashayekhi discloses (Col.7 Lines 43 - 45);
performing an integrity check on the data (Col.4 Lines 1 - 3).

As per Claim 20, Baser discloses that

detecting a security operation tag in a header to the data (Col.3 Line 50 and Col.9 Lines 30 - 32);
detecting failure of an integrity check (Col.4 Lines 1 - 3);

As per Claim 27, Baser discloses that

receiving data from a network application program interface (API) (Col.35 Lines 23 - 25);

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data (Col.22 Lines 50 - 52);

create a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association (Col.3 Lines 22 - 29);

send the data to which the security operation has been applied to a network protocol layer (Col.28 Lines 32 - 33).

Baser does not disclose that applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data. However, Mashayekhi discloses applying the security operation to the data (Col.3 Lines 37 - 39). Therefore, it would have been obvious to a

person of ordinary skill in the art to implement the claimed invention by applying the security operation using the security association as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

As per Claim 28, Baser discloses that a processing unit to:
receive data from a network protocol layer (Col.35 Lines 23 - 25);
[[to]] determine if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data (Col.22 Lines 50 - 52);
create a selector based on the selector data, said selector indicating at least a portion of the data and a security association (Col.3 Lines 22 - 29);

Baser does not disclose that applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data. However, Mashayekhi discloses applying the security operation to the data (Col.3 Lines 37 - 39). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by applying the security operation using the security association as taught by Mashayekhi. Such modifications would have been obvious because by combining the teachings of Baser and Mashayekhi, the data can be more secure.

[[to]] send the data to which the security operation has been applied to a network application program interface (API) (Col.28 Lines 32 - 33).

Conclusion

4. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C.

20231 or faxed to: (703) 872-9306 for all formal communications.

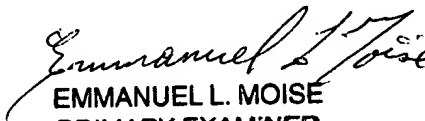
Hand-delivered responses should be brought to Crystal Park II, 2121
Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications
from the examiner should be directed to Pramila Parthasarathy whose
telephone number is 703-305-8912. The examiner can normally be
reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the
examiner's supervisor, Albert Decady can be reached on 703-305-9595.
The fax phone number for the organization where this application or
proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this
application or proceeding should be directed to the receptionist whose
telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912


EMMANUEL L. MOISE
PRIMARY EXAMINER
Art 2136

January 14, 2004